IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	)	
	)	
Plaintiff,	)	Civil Action No. 16-1780
	)	
v.	)	The Honorable Arthur J. Schwab
	)	Senior United States District Judge
"flux"	)	
a/k/a "ffhost",	)	
	)	
and	)	
	)	
"flux2"	)	
a/k/a "ffhost2",	)	
	)	
Defendants.	)	

MOTION FOR PERMANENT INJUNCTION

Plaintiff, the United States of America, by and through its attorneys, Scott W. Brady, United States Attorney for the Western District of Pennsylvania, Jennifer R. Andrade, Assistant United States Attorney, Brian Benczkowski, Assistant Attorney General, and Cristina M. Posa, Senior Counsel, respectfully moves this Court, *ex parte*, to issue a permanent injunction in this matter against Defendants "flux" and "flux2."

1. On December 9, 2016, this Honorable Court issued a Preliminary Injunction on the motion of counsel for the United States that was designed to prevent the fraud being perpetrated on hundreds of thousands of victims world-wide by the defendants. (Dkt. No. 17).

2. The defendants administered a hosting infrastructure known as "Avalanche" comprised of a worldwide network of servers controlled by and through a highly organized central control system. The Avalanche administrators rented out access to the Avalanche network to cyber criminals for the bulletproof hosting services over which the malware attacks and money mule campaigns victimized hundreds of thousands of people throughout the world.

3. The injunctive relief Ordered by this Honorable Court on December 9, 2016, commanded the defendants to stop using Avalanche to defraud and wiretap American citizens and businesses. To give effect to that prohibition, this Honorable Court authorized the United States to employ a series of technical measures, referred to herein as the "sinkholing operation," designed to disrupt the defendants' hosting infrastructure and related malware systems. Specifically, this Honorable Court authorized the United States to: (1) direct certain U.S. Domain Registries to redirect a list of domain names used by Avalanche or the malware systems that traverse it to substitute servers and, at the registries' discretion, transfer the domain names to the Registry of Last Resort (RoLR); (2) direct certain U.S. Domain Registries to cause a separate list of domain names to block access to a proscribed list of domain names used by Avalanche or the malware systems that traverse it and, at the registries' discretion, to register those with the Registry of Last Resort (RoLR); (3) direct certain U.S. Domain Registries to register a proscribed list of domain names, direct them to substitute servers, and, at the registries' discretion, transfer the domain names to the Registry of Last Resort (RoLR); and (4) direct certain U.S. Domain Registries to transfer a proscribed list of domain names and redirect them to substitute servers. (Dkt. No. 17).

4. In addition to the relief described above, this Honorable Court also authorized the United States to utilize a Pen Register/Trap and Trace Order that collects the dialing, routing, addressing, and signaling information of communications sent by the computers infected with Avalanche or the malware systems that traverse it to the substitute servers and other computer infrastructure established pursuant to the TRO sought by the Government. This information is disseminated to the Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT), the ShadowServer Foundation, the Fraunhofer Institute for

Communication, Information Processing and Ergonomics (FKIE) to facilitate the notification of Avalanche victims and provide instruction on how to remove these infections from their computers.

5. At the time this Honorable Court granted the equitable relief, the United States advised this Honorable Court that, if the United States sought to have the sinkholing operation extend beyond one year, it would submit to this Honorable Court a request to continue the sinkholing operation.

6. On November 27, 2017, the United States filed a motion with the Court to continue the equitable relief originally ordered in December of 2016, including the sinkholing operation. (Dkt. No. 26). On November 28, 2017, this Honorable Court granted the United States' motion. (Dkt. No. 27).

7. On November 23, 2018, the United States again filed a motion with the Court to continue the equitable relief, including the sinkholing operation. (Dkt. Nos. 17, 29). On November 26, 2018, this Honorable Court granted the United States' request. (Dkt. No. 30).

8. Attached is the Declaration of Special Agent Brian Stevens which sets forth a summary of the takedown of the Avalanche infrastructure, the present status of the ongoing sinkholing operation, as well as the factual basis for the relief sought. In particular, as described in Special Agent Stevens' Declaration, Gennady Kapkanov, a 35 year-old Ukrainian citizen living in Poltava, Ukraine, is believed to be involved as an administrator for the Avalanche Infrastructure, and to have used the online monikers "flux" and "ffhost." Kapkanov was arrested in February 2018 and indicted by a Grand Jury sitting in the Western District of Pennsylvania on April 17, 2019. *See* Crim. A. No. 19-104 (W.D. Pa.).

9. The Government now seeks an Order of Permanent Injunction to permanently restrain and enjoin the Defendants from using malicious software or code in furtherance of any scheme to commit wire fraud, bank fraud, or to engage in unauthorized interception of electronic communications, and to prohibit Defendants from running, controlling, or communicating with software known as Andromeda, Corebot, GetTiny, Gozi2, KINS, Matsnu, Nymaim/Goznym, Ranbyus, Rovnix, TeslaCrypt, Tiny Banker aka Tinba, Trusteer App, UrlZone, VM Zeus, Vawtrak, and Xswkit, on any computers not owned by the Defendants.

10. To that end, the Government respectfully requests that the Court enter the attached proposed order which details actions to be taken to effectuate the permanent injunction with respect to the sinkholing operation.

11. As no one has yet entered an appearance on behalf of the Defendants, including over the past year, the United States respectfully requests that this Honorable Court consider and, if it deems appropriate, grant the requested relief forthwith, without any provision of time for a response from entities that have not entered an appearance or sought to engage either the United States or this Honorable Court.

Respectfully submitted,

SCOTT W. BRADY
United States Attorney

By: /s/ Jennifer Andrade
JENNIFER ANDRADE
Assistant U.S. Attorney
Western District of Pennsylvania
U.S. Post Office & Courthouse
700 Grant Street, Suite 4000
Pittsburgh, PA 15219
(412) 894-7426 Phone
(412) 644-4549 Fax
PA ID No. 94685
Jennifer.Andrade@usdoj.gov

BRIAN BENCZKOWSKI
Assistant Attorney General

By: /s/ Cristina M. Posa
CRISTINA M. POSA
Senior Counsel
U.S. Department of Justice
Criminal Division
Computer Crime and Intellectual Property Section
1301 New York Ave., NW, Suite 600
Washington, DC 20003
(202) 598-6383 Phone
(202) 514-6113 Fax
NY Bar Registration No. 3986098
cristina.posa@usdoj.gov